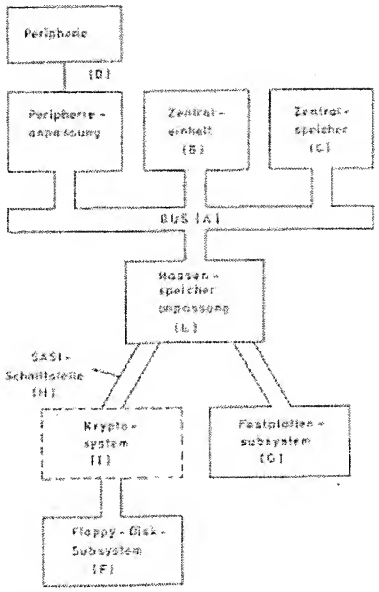
Digital computer

Publication number: DE3613827 (A1)
Publication date: 1987-10-29
Inventor(s): WEBER WOLFGANG PROF DR ING [DE]
Applicant(s): WEBER WOLFGANG PROF DR ING
Classification:
- international: ***G06F21/00;*** *G06F1/00;* **G06F21/00;** G06F1/00; (IPC1-7): H04L9/00; G06F12/14
- European: G06F21/00N1C1; G06F21/00N1D2; G06F21/00N9A2; G06F21/00N9T
Application number: DE19863613827 19860424
Priority number(s): DE19863613827 19860424

Abstract of **DE 3613827 (A1)**

The invention concerns a digital computer with a central unit (B) and at least one external mass memory (F), which is connected via a mass memory adapter (E) and a data line to the central unit (B). In such a digital computer, to encrypt all the data which is stored on the external mass memory automatically so that it is as secure as possible against access, without requiring additional computer time within the central unit, the invention proposes that a microcomputer (I) should be connected into the data line between the mass memory adapter (E) and the external mass memory (F), and that this microcomputer (I) should encrypt the data on the way from the central unit (B) to the external mass memory (F), and decrypt it on the way from the external mass memory (F) to the central unit (B).



(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(11) **DE 36 13 827 A1**

(51) Int. Cl. 4:
G 06 F 12/14
// H04L 9/00

(21) Aktenzeichen: P 36 13 827.4
(22) Anmeldetag: 24. 4. 86
(43) Offenlegungstag: 29. 10. 87

DE 36 13 827 A1

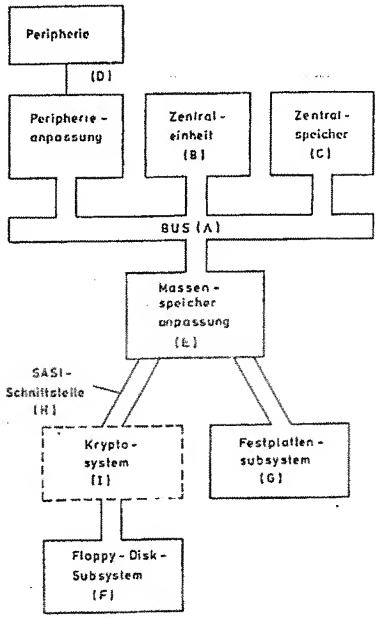
(71) Anmelder:
Weber, Wolfgang, Prof. Dr.-Ing., 4630 Bochum, DE

(74) Vertreter:
Behrendt, A., Dipl.-Ing., Pat.-Anw., 4630 Bochum

(72) Erfinder:
gleich Anmelder

(54) Digitalrechner

Die Erfindung betrifft einen Digitalrechner mit einer Zentraleinheit (B) und mindestens einem externen Massenspeicher (F), der über eine Massenspeicheranpassung (E) und eine Datenleitung an die Zentraleinheit (B) angeschlossen ist. Um bei einem solchen Digitalrechner alle auf dem externen Massenspeicher abgespeicherten Daten automatisch weitestgehend zugriffssicher zu verschlüsseln, ohne daß zusätzliche Rechnerzeit im Bereich der Zentraleinheit benötigt wird, schlägt die Erfindung vor, daß in die Datenleitung zwischen der Massenspeicheranpassung (E) und dem externen Massenspeicher (F) ein Mikrorechner (I) eingeschaltet ist, der die Daten auf dem Weg von der Zentraleinheit (B) zum externen Massenspeicher (F) chiffriert und auf dem Weg vom externen Massenspeicher (F) zur Zentraleinheit (B) dechiffriert.



DE 36 13 827 A1

Patentansprüche

1. Digitalrechner, mit einer Zentraleinheit (*B*) und mindestens einem externen Massenspeicher (*F*), der über eine Massenspeicheranpassung (*E*) und eine Datenleitung an die Zentraleinheit (*B*) angeschlossen ist, **dadurch gekennzeichnet,** daß in die Datenleitung zwischen der Massenspeicheranpassung (*E*) und dem externen Massenspeicher (*F*) ein Mikrorechner *(I)* eingeschaltet ist, der die Daten auf dem Weg von der Zentraleinheit (*B*) zum externen Massenspeicher (*F*) chiffriert und auf dem Weg von dem externen Massenspeicher (*F*) zur Zentraleinheit (*B*) dechiffriert.

2. Digitalrechner nach Anspruch 1, dadurch gekennzeichnet, daß der zur Chiffrierung und Dechiffrierung dienende Mikrorechner *(I)* in die Schnittstelle (*H*) zwischen der Massenspeicheranpassung (*E*) und dem externen Massenspeicher (*F*) integriert ist.

3. Digitalrechner nach den Ansprüchen 1 und 2, dadurch gekennzeichnet, daß der zur Chiffrierung und Dechiffrierung dienende Mikrorechner *(I)* mit einer Magnetkartenlesestation (*K*) zur Eingabe von unterschiedlichen Chiffrierschlüssels versehen ist.

Beschreibung

Die Erfindung betrifft einen Digitalrechner mit einer Zentraleinheit und mindestens einem externen Massenspeicher, der über eine Massenspeicheranpassung und eine Datenleitung an die Zentraleinheit angeschlossen ist.

Ein Problem bei derartigen Digitalrechnern besteht darin, daß die in dem externen Massenspeicher abgelegten Daten und/oder Programme von unberechtigten Personen gelesen, entwendet oder manipuliert werden können. Dies gilt insbesondere, wenn der externe Massenspeicher auswechselbare Datenträger hat, wie zum Beispiel ein Floppy-Disc-Massenspeicher.

Nach dem Stande der Technik ist bekannt, den unbefugten Zugang zu diesen Daten durch einen Paßwortschutz zu unterbinden. Dieser Paßwortschutz ist jedoch für einen Fachmann verhältnismäßig leicht umgehbar. Weiterhin sind Verfahren bekannt, die mit Hilfe eines Softwaresystems, das heißt also durch einen in der Zentraleinheit selbst ablaufenden Algorithmus, auf Anforderung des Benutzers die auf dem Massenspeicher zu speichernden Daten zu verschlüsseln. Bei entsprechender Wahl von geeigneten Verschlüsselungsalgorithmen läßt sich hierdurch zwar eine große Sicherheit erzielen. Diese Verschlüsselung hat jedoch den Nachteil, daß für das Chiffrieren und Dechiffrieren verhältnismäßig viel Rechnerzeit der Zentraleinheit verbraucht wird. Außerdem ist es in diesem Fall notwendig, das entsprechende Chiffrierprogramm expliziert zu starten und zum Ablauf zu bringen, so daß sich insofern weitere Manipulationsmöglichkeiten eröffnen.

Aufgabe der Erfindung ist es, den Digitalrechner der eingangs genannten Art dahingehend weiterzubilden, daß alle auf dem externen Massenspeicher abgespeicherten Daten automatisch weitestgehend zugriffssicher verschlüsselt werden, ohne daß zusätzliche Rechnerzeit im Bereich der Zentraleinheit benötigt wird.

Zur Lösung dieser Aufgabe schlägt die Erfindung ausgehend von einem Digitalrechner der eingangs genannten Art vor, daß in die Datenleitung zwischen der Massenspeicheranpassung und dem externen Massenspeicher ein Mikrorechner eingeschaltet ist, der die Daten auf dem Weg von der Zentraleinheit zum externen Massenspeicher chiffriert und auf dem Weg vom externen Massenspeicher zur Zentraleinheit dechiffriert.

Der Digitalrechner gemäß der Erfindung hat den Vorteil, daß alle Daten auf dem Weg zwischen der Zentraleinheit und dem externen Massenspeicher zwangsläufig den zur Chiffrierung und Dechiffrierung dienenden Mikrorechner durchlaufen müssen, so daß in keinem Fall unchiffrierte Daten in den externen Massenspeicher gelangen können. Dadurch, daß der zur Chiffrierung und Dechiffrierung dienende Mikrorechner im Parallelbetrieb zur Zentraleinheit arbeitet, geht die für die Chiffrierung und Dechiffrierung benötigte Rechenzeit zu Lasten dieses Mikrorechners, nicht aber zu Lasten der Zentraleinheit. Im Bereich der Zentraleinheit geht also durch diese zusätzliche Maßnahme keine Rechnerzeit verloren. Da die für die Chiffrierung und Dechiffrierung benötigte Rechenzeit bei Verwendung eines Mikrorechners im Zehntelsekundenbereich liegt, sind die auftretenden Verzögerungen für den Benutzer des externen Massenspeichers hinnehmbar.

Die Verwendung eines Mikrorechners für die Chiffrierung und Dechiffrierung gestattet es ohne weiteres, einen Chiffrieralgorithmus zu verwenden, der eine sehr große Zahl von Kombinationen zuläßt, so daß die unbefugte Entschlüsselung außerordentlich schwierig wird. So ist es beispielsweise ohne weiteres möglich, einen Chiffrieralgorithmus zu verwenden, der 10 exp 9 Variationen zuläßt. Ein anderer Vorteil der erfindungsgemäßen Verwendung des Mikrorechners liegt darin, daß die Menge der Daten durch die Chiffrierung unverändert bleiben kann. Der Mikrorechner kann eine gegebene Menge von Daten in die gleiche Menge chiffrierter Daten überführen, wobei der Chiffrierschlüssel selbst nicht Bestandteil der abgespeicherten Daten ist. Für die Abspeicherung der chiffrierten Daten wird also kein zusätzlicher Speicherraum benötigt. Schließlich erfordert das Verschlüsselungssystem gemäß der Erfindung keine Eingriffe in die Betriebssoftware des Digitalrechners. Die Einfügung des Mikrorechners in den Datenpfad zum externen Massenspeicher wird von der Zentraleinheit nicht wahrgenommen; die Zentraleinheit arbeitet mit dem externen Massenspeicher zusammen, als ob das Verschlüsselungssystem nicht vorhanden sei. Das Verschlüsselungssystem gemäß der Erfindung eignet sich somit auch besonders gut zur Nachrüstung von vorhandenen Digitalrechnern.

Eine besonders bevorzugte Ausführungsform des Digitalrechners gemäß der Erfindung sieht vor, daß der zur Chiffrierung und Dechiffrierung dienende Mikrorechner in die Schnittstelle zwischen der Massenspeicheranpassung und dem externen Massenspeicher integriert ist. Durch die Erweiterung dieser Schnittstelle mit dem Mikrorechner ist es möglich, eine vorhandene digitale Rechenanlage nachträglich mit dem Verschlüsselungssystem gemäß der Erfindung zu versehen.

Zweckmäßig ist es weiterhin den zur Chiffrierung und Dechiffrierung dienenden Mikrorechner mit einer Magnetkartenlesestation zur Eingabe von unterschiedlichen Chiffrierschlüsseln zu versehen. Hierdurch ist es beispielsweise möglich, dem Inhaber einer bestimmten Magnetkarte nur bestimmte Daten zugänglich zu machen. Außerdem ist es möglich, beispielsweise eine hierarchisch gegliederte Zugriffsstruktur zu schaffen, mit der die Zugriffserlaubnis zu einzelnen Datensätzen oder Programmen entsprechend der Betriebshierarchie (einfache Mitarbeiter, Gruppenleiter, Abteilungsleiter etc.)

gegliedert werden kann.

Ein Ausführungsbeispiel der Erfindung wird im folgenden anhand der Zeichnung näher erläutert. Es zeigen:

Fig. 1 Ein Blockschaltbild eines Digitalrechners gemäß der Erfindung;

Fig. 2 eine abgewandelte Ausführungsform des Digitalrechners gemäß der Erfindung im Bereich des zusätzlichen Mikrorechners.

Die in **Fig. 1** mit *BUS (A)* bezeichneten Verbindungsleitungen, die Zentraleinheit (*B*), der Zentralspeicher (*C*), die Peripherieanpassung mit Peripherie (*D*), die Massenspeicheranpassung (*E*) mit dem als externer Speicher dienenden Floppy-Disc-Subsystem (*F*) und optional Festplatten-Subsysteme (*G*) gehören standardgemäß zur Ausrüstung eines Digitalrechners, insbesondere eines Personal-Computers. Die Schnittstelle (*H*) zwischen der Massenspeicheranpassung (*E*) und dem als externen Massenspeicher dienenden Floppy-Disc-Subsystem (*F*) genügt dem SASI-Standard (SASI = Shugart Ass. Standard Interface ist eine Firmennorm der Firma Shugart Association). Diese Schnittstelle (*H*) ist durch Auftrennung und Einbau eines Mikrorechners *(I)* erweitert. Dieser Mikrorechner *(I)* wandelt alle dem als externen Speicher dienenden Floppy-Disc-Subsystem (*F*) zuzuführenden Daten automatisch und ohne Zutun des Benutzers in eine Form, die es einem nichtauthorisierten Benutzer praktisch unmöglich macht, die Daten zu interpretieren. Die Chiffrierung ist reversibel, daß heißt beim Rücktransport der Daten von dem externen Speicher (Floppy-Disc-Subsystem *F*) zur Zentraleinheit (*B*) zum Zwecke der weiteren Bearbeitung wandelt der Mikrorechner *(I)* die Daten in den Originalzustand zurück. Für diese Umwandlungen benötigt der Mikrorechner lediglich eine Rechenzeit im Bereich von Zehntelsekunden.

Wie sich aus **Fig. 2** ergibt, kann der Mikrorechner *(I)* gegebenenfalls mit einer Magnetkartenlesestation (*K*) verbunden sein. Der Verschlüsselungsalgorithmus der von *(E)* nach *(F)* übertragen und der von *(F)* nach *(E)* zurückübertragenen Daten ist in einem Festwertspeicher des Mikrorechners *(I)* abgelegt. Der zur Chiffrierung und Dechiffrierung verwendete Benutzerschlüssel wird zu Beginn des Dialoges mit dem Digitalrechner einmal über die Magnetkartenstation *(K)* eingelesen.

– Leerseite –

3613827

Nummer: 36 13 827
Int. Cl.[4]: G 06 F 12/14
Anmeldetag: 24. April 1986
Offenlegungstag: 29. Oktober 1987

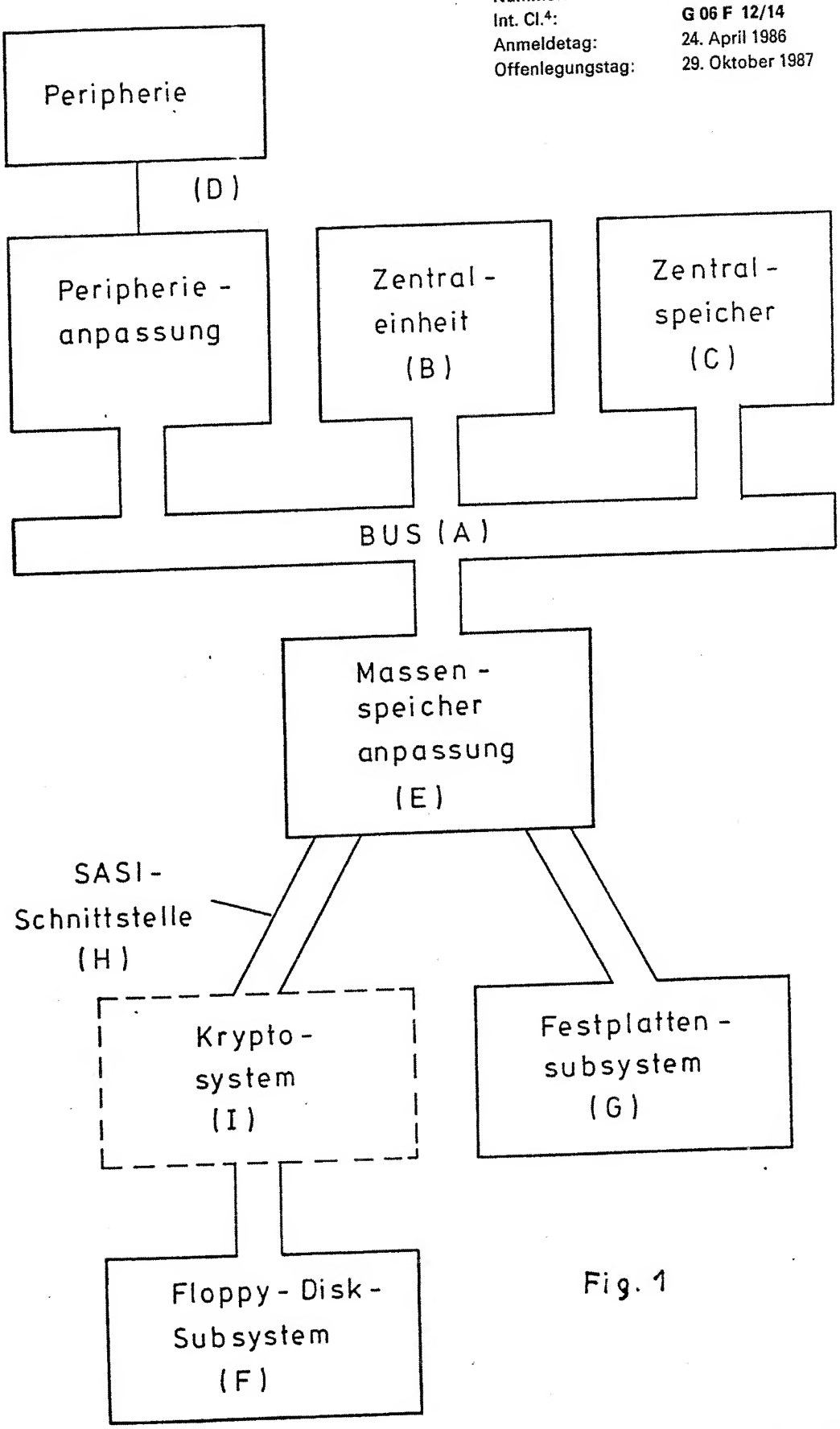


Fig. 1

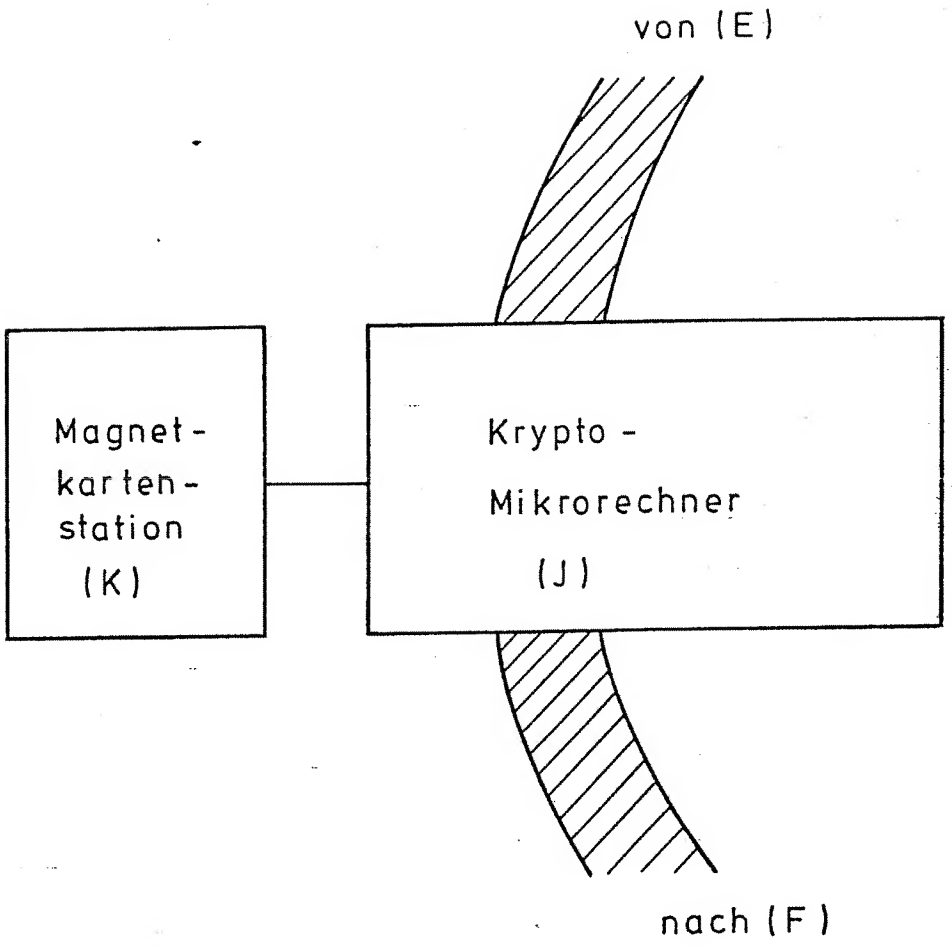


Fig. 2